

**POWER ALLOCATION, RELAY SELECTION
& COOPERATIVE TECHNIQUES FOR
PHYSICAL LAYER SECURITY IN RELAYED
COMMUNICATION SYSTEMS**

SARBANI GHOSE



**DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI**

April, 2017

©Indian Institute of Technology Delhi (IITD), New Delhi, 2017

**POWER ALLOCATION, RELAY SELECTION
& COOPERATIVE TECHNIQUES FOR
PHYSICAL LAYER SECURITY IN RELAYED
COMMUNICATION SYSTEMS**

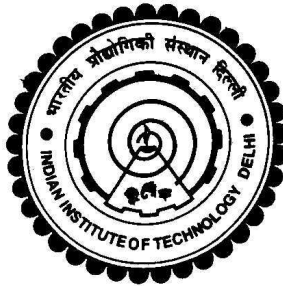
by

SARBANI GHOSE

Department of Electrical Engineering

Submitted

in fulfillment of the requirements of the degree of **Doctor of Philosophy**
to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI

APRIL, 2017

Certificate

This is to certify that the thesis entitled “**Power Allocation, Relay Selection & Cooperative Techniques for Physical Layer Security in Relayed Communication Systems**” being submitted by Ms. **Sarbani Ghose** to the Department of Electrical Engineering, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is the record of the bona-fide research work carried out by her under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other university or institute for the award of any degree or diploma.

Date: (Dr. Ranjan Bose)

Place: Professor

Department of Electrical Engineering
Indian Institute of Technology Delhi
Hauz Khas, New Delhi 110016

Acknowledgements

To start with, I wish to express my deep gratitude to my supervisor Professor Ranjan Bose. He has been a source of constant encouragement and always gave me the best support. He instilled into me the motivation for learning the new techniques and the unique methodologies to keep oneself abreast of the latest technological developments in the fast growing scenario. I am deeply indebted to my student research committee members Professors Manav Bhatnagar, Vinay Joseph Ribeiro, and Brejesh Lall, for many a useful interactions and for their kind comments and suggestions which were always useful and fulfilling.

I gratefully acknowledge all the expert guidance from the professors at the IIT Delhi from whom I have benefited a lot during the courses. I offer my regards to all members of the Research Scholar Lab, who supported me in all respect during the completion of the Ph.D. Most importantly, my heartfelt gratitude is for my father Sudipta Ghose who always supported me in all my academic pursuits and encouraged me to do my best. I would also like to thank my husband Anirban Kundu for his unflinching support and loving encouragement.

Sarbani Ghose

Abstract

Wireless networks are broadcast in nature. Hence wireless transmission can be heard by multiple receivers with different signal strengths. With the help of a ‘friendly jammer’, we can create confusion at the eavesdropper. That brings us to a design problem, that is how to fulfill rate requirement of secure communication with a constraint on the resources i.e. the transmit power. In this thesis, we first propose how to design optimal weight at the friendly jammer such that the overall secrecy rate is maximized, under the constraint of total power. We obtain expressions for optimal source power that maximizes secrecy rate. We find that beyond a region, it is better to rely on direct transmission and within the region jamming is effective. We term this region as ‘effective region for jamming’. Similar region is found when we aim at minimizing total transmit power, with a constraint on secrecy rate. It is observed that the secrecy rate improves in a less cluttered environment. After inclusion of the fading model, it is observed that the secrecy rate improves, for two particular cases i.e. mobile eavesdropper and mobile jammer. Thus, fading helps to improve secrecy.

Relaying can expand the coverage area of communication and offer diversity gains. With the help of a relay, a positive secrecy capacity can be achieved which is otherwise zero when relay is not being used. Next, we propose an adaptive scheme that combines the merits of both decode-and-forward (DF) and amplify-and-forward (AF) scheme. If the signal-to-noise ratio (SNR) of first hop is below a certain prescribed threshold, then AF is adopted and beyond a threshold DF is employed. We find that at low secrecy rate, to achieve same secrecy performance

hybrid decode-and-forward (HDAF) requires higher SNR as compared to the case of higher secrecy rate. A fixed ‘least secrecy outage’ is obtained depending on input parameters. When the destination and eavesdropper both employ maximal ratio combining (MRC) receiver, we have derived a closed-form expression for secrecy outage probability (SOP) of this system. Also asymptotic performance of HDAF scheme is obtained. It is seen that the effect on unbalance is more pronounced at lower secrecy rate as compared to higher rate.

Secrecy capacity can be improved by selecting a single relay that ensures best transmission link to the destination and worst link to the wiretapper. Considering a network with multiple AF relays, we solve joint power allocation and optimal relay selection problem. When source transmits message signal, destination sends jamming signal concurrently. Closed-form expression of SOP of an optimal relay selection based on destination jamming has been derived. Relay selection schemes are formulated based on instantaneous, statistical channel state information (CSI) of the eavesdropper. It has been seen secrecy outage is worst when relay selection is performed without taking into account jamming, in the presence of eavesdropper.

In a multi-node relaying network, the intended channel quality can be enhanced through the collaboration of relays, which exploits the spatial diversity by relays at the transmitter and/or the receiver. Multiple relays can cooperate to combine redundant copies of the same signal, hence achieve a diversity gain. In this thesis, we analyze the secrecy performance of a single relay-based dual-hop communication systems with diversity combining a) at the eavesdropper only, b) at the destination and the eavesdropper. We find that secrecy performance is the best, when the relay is able to decode the message perfectly. It is observed that the availability of channel state information (CSI) can only help to improve secrecy when secrecy rate is low. It is also observed that unbalances created by imposing constraint on either of the source-relay or relay-destination average SNR does not yield similar performance.

सार

वायरलेस नेटवर्क प्रकृति में प्रसारित किए जाते हैं। इसलिए बेतार संचरण अलग सिग्नल क्षमताओं के साथ कई रिसेवर से सुना जा सकता है। एक 'अनुकूल जैमर' की मदद से, हम छिपकर बातें सुनेवाला पर भ्रम की स्थिति पैदा कर सकते हैं। यही कारण है कि एक डिजाइन समस्या के लिए हमें लाता है, कि एक बाधा के साथ सुरक्षित संचार की दर की आवश्यकता को पूरा करने के लिए कैसे संसाधनों अर्थात् संचारित शक्ति पर है। इस शोध में, हम पहले प्रस्ताव कैसे अनुकूल जैमर पर इष्टतम वजन डिजाइन करने के लिए इस तरह के हैं कि समग्र गोपनीयता दर बढ़ा किया गया है कुल बिजली की कमी के तहत,। हम इष्टतम स्रोत शक्ति है कि गोपनीयता दर अधिकतम के लिए अभिव्यक्ति प्राप्त करते हैं। हम पाते हैं कि एक क्षेत्र से बाहर है, यह सीधा प्रसारण पर और भीतर क्षेत्र ठेला प्रभावी है भरोसा करने के लिए बेहतर है। हम 'प्रभावी रूप से इस क्षेत्र में पद ठेला के लिए इस क्षेत्र'। जब हम गोपनीयता दर पर एक बाधा के साथ, कुल संचारित शक्ति को कम करने का उद्देश्य इसी प्रकार क्षेत्र पाया जाता है। यह देखा गया है कि गोपनीयता दर अव्यवस्था कम वातावरण में सुधार। फिटिंग मॉडल के शामिल किए जाने के बाद, यह पाया गया है कि गोपनीयता दर, बेहतर बनाता है दो विशेष मामलों मोबाइल छिपकर बातें सुनेवाला और मोबाइल जैमर अर्थात्। इस प्रकार, लुप्त होती गोपनीयता सुधार करने के लिए मदद करता है।

प्रसारण संचार के कवरेज क्षेत्र का विस्तार और विविधता लाभ की पेशकश कर सकते हैं। एक रिले की मदद से, एक सकारात्मक गोपनीयता क्षमता प्राप्त किया जा सकता है जो अन्यथा शून्य है जब रिले का उपयोग नहीं किया जा रहा है। इसके बाद, हम एक अनुकूली योजना है कि दोनों डिकोड-एंड-फॉरवर्ड (डीफ) और एम्पलीफी-एंड-फॉरवर्ड (आफ) योजना की खूबियों को जोड़ती प्रस्ताव करते हैं। संकेत से शोर अनुपात (असनर) पहले हॉप की एक निश्चित निर्धारित सीमा से नीचे है, तो वायुसेना अपनाया है और एक सीमा से परे डीफ कार्यरत है। हम कम गोपनीयता दर पर, प्राप्त करने के लिए है कि एक ही गोपनीयता प्रदर्शन संकर डिकोड-एंड-फॉरवर्ड (अच्छीफ) उच्च असनर की आवश्यकता है उच्च गोपनीयता दर के मामले की तुलना में पाते हैं। एक निश्चित 'कम से कम गोपनीयता आउटटेज' इनपुट पैरामीटर के आधार पर प्राप्त की है। गंतव्य और छिपकर बातें सुनेवाला दोनों अधिक से अधिक अनुपात को रोजगार जब संयोजन (एमआरसी) रिसेवर, हम इस प्रणाली की गोपनीयता आउटटेज संभावना (एसओपी) के लिए एक पूर्ण-सूत्र अभिव्यक्ति ली गई है। इसके अलावा अच्छीफ योजना के असिम्प्टोटिक प्रदर्शन प्राप्त की है। यह देखा गया है कि असंतुलित पर प्रभाव कम गोपनीयता दर से और अधिक स्पष्ट उच्च दर की तुलना में है।

गोपनीयता क्षमता एक भी रिले कि गंतव्य के लिए सबसे अच्छा ट्रांसमिशन लिंक और छिपकर बातें सुनेवाला लिए सबसे खराब लिंक सुनिश्चित करता है का चयन करके सुधार किया जा सकता। कई वायुसेना रिले के साथ एक नेटवर्क को देखते हुए, हम संयुक्त शक्ति आवंटन और इष्टतम रिले चयन समस्या का समाधान। स्रोत संदेश संकेत पहुंचाता है, गंतव्य समवर्ती संकेत जाम भेजती है। गंतव्य ठेला के आधार पर एक इष्टतम रिले चयन के एसओपी का पूर्ण-सूत्र अभिव्यक्ति प्राप्त किया गया है। रिले चयन योजनाओं छिपकर बातें सुनेवाला की तात्कालिक, सांख्यिकीय चैनल राज्य सूचना (सीएसआई) के आधार पर तैयार की जाती हैं। यह देखा गया है गोपनीयता आउटेज सबसे खराब जब रिले चयन छिपकर बातें सुनेवाला की उपस्थिति में, खाते ठेला में लेने के बिना किया जाता है |

एक बहु नोड रिले नेटवर्क में, इरादा चैनल गुणवत्ता रिले का सहयोग है, जो ट्रांसमीटर और / या रिसेवर पर रिले द्वारा स्थानिक विविधता कारनामे के माध्यम से बढ़ाया जा सकता है। एकाधिक रिले एक ही संकेत की अनावश्यक प्रतियां गठबंधन है, इसलिए एक विविधता लाभ प्राप्त करने में सहयोग कर सकते हैं। इस शोध में, हम विविधता गंतव्य और छिपकर बातें सुनेवाला पर छिपकर बातें सुनेवाला केवल, ख) में एक संयोजन) के साथ एक एकल रिले-आधारित दोहरे हॉप संचार प्रणाली की गोपनीयता के प्रदर्शन का विश्लेषण। हम पाते हैं कि गोपनीयता प्रदर्शन, सबसे अच्छा है जब रिले पूरी तरह से संदेश को डिकोड करने में सक्षम है। यह देखा गया है कि चैनल राज्य सूचना (सीएसआई) की उपलब्धता केवल गोपनीयता बेहतर बनाने में मदद कर सकते हैं जब गोपनीयता दर कम है। यह भी देखा गया है कि स्रोत-रिले या रिले-गंतव्य औसत असनर में से किसी पर बाधा भव्य इसी तरह के प्रदर्शन की उपज नहीं है के द्वारा बनाई गई असंतुलन कि।

Contents

Certificate	i
Acknowledgements	iii
Abstract	v
List of Figures	xiii
List of Tables	xvii
List of Abbreviations	xix
1 Introduction	1
1.1 Introduction	1
1.2 Wireless Channels	2
1.2.1 Rayleigh Fading Channel Model	5
1.3 Physical Layer Security (PLS)	5
1.3.1 Wiretap Channel	7
1.3.2 Gaussian Signaling	8
1.3.3 Performance Metrics of Secrecy	9
1.4 Relaying Techniques	11
1.4.1 Amplify-and-Forward (AF)	12
1.4.2 Decode-and-Forward (DF)	13
1.4.3 Cooperative Jamming (CJ)	13
1.5 Cooperative Diversity	14

1.5.1	Maximal Ratio Combining (MRC)	14
1.5.2	Equal Gain Combining (EGC)	14
1.5.3	Selection Combining (SC)	15
1.6	Motivation	15
1.7	Contributions	16
1.8	Organization of Thesis	18
2	Related work	23
2.1	Ergodic Secrecy Rate (ESR)	23
2.2	Secrecy Outage Probability (SOP)	24
2.3	Beamforming	26
2.4	Friendly Jamming	28
2.4.1	External Jammer	28
2.4.2	Source, Destination Assisted Jamming	29
2.5	Power Allocation in Relayed Communication	30
2.5.1	Based on Multi-antenna:	31
2.5.2	Based on Hops:	31
2.6	Cooperative Secure Communication	33
2.7	Summary	34
3	Beamformer Design to Maximize Secrecy Rate under Path-Loss and Rayleigh Fading	37
3.1	Introduction	37
3.2	System Model	39
3.3	Optimal Design of Weight and Power Allocation to Maximize Secrecy Rate	40
3.4	Numerical Results	44
3.5	Summary	48
4	Beamformer Design to Maximize Secrecy Rate and Minimize Total Transmit Power under Correlated Fading	49

4.1	Introduction	49
4.2	System Model and Secrecy Rate Formulation	51
4.3	Closely Located Antenna Elements	54
4.4	System Design	55
4.4.1	Secrecy Rate Maximization (SRM)	55
4.4.2	Transmit Power Minimization (TPM)	59
4.5	Simulation Results and Discussion	63
4.5.1	Simulation Setup	63
4.5.2	SRM	64
4.5.3	TPM	66
4.6	Summary	67
5	Secrecy Performance of a Hybrid Decode-Amplify-Forward Relay Network	71
5.1	Introduction	71
5.2	System Model	72
5.3	Secrecy Outage Probability Analysis	73
5.4	Asymptotic Analysis	76
5.4.1	Balanced Case	77
5.4.2	Unbalanced Case	78
5.5	Numerical Results	78
5.6	Summary	82
6	Relay Selection in dual-hop AF Relay Networks using Destination Assisted Jamming	83
6.1	Introduction	83
6.1.1	Related Prior Work	84
6.2	System and Channel Models	85
6.2.1	Received SNRs at D and E	87
6.2.2	Problem Decomposition and Optimization	88

6.3	Optimal Power Allocation	89
6.4	Secrecy Outage Analysis of Different Relay Selection Strategies . . .	90
6.4.1	Optimal Selection	90
6.4.2	Conventional Selection with Jamming (CS)	91
6.4.3	Conventional Selection without Jamming (CS-NJ)	94
6.4.4	Sub-optimal Selection (SS)	95
6.5	Numerical Results	96
6.6	Summary	97
7	Secrecy Performance of Dual-hop DF Relay System with Diversity Combining at the Eavesdropper	99
7.1	Introduction	99
7.2	System Model	101
7.3	Secrecy Outage Probability (SOP)	103
7.3.1	Knowledge of CSI is not Available at Transmitter	104
7.3.2	Complete Knowledge of CSI at Transmitter	109
7.4	Ergodic Secrecy Rate (ESR)	111
7.4.1	Knowledge of CSI is not Available at Transmitter	112
7.4.2	Complete Knowledge of CSI at Transmitter	113
7.5	Asymptotic Analysis	115
7.5.1	Balanced Case	116
7.5.2	Unbalanced Case I	118
7.5.3	Unbalanced Case II	120
7.6	Numerical Results	122
7.7	Summary	128
8	Secrecy Performance of Diversity Schemes for Dual-hop Regenerative System with Diversity Combining at the Destination and Eavesdropper	129
8.1	Introduction	129

8.2	System Model	131
8.3	Mathematical Preliminaries	133
8.4	SOP of Various Combination of Diversity Combining Schemes . . .	134
8.4.1	Non availability of CSI at Transmitter	135
8.4.2	Complete Knowledge of CSI at Transmitter	137
8.5	Ergodic Secrecy Rate	138
8.5.1	Non availability of CSI at Transmitter	138
8.5.2	Complete Knowledge of CSI at Transmitter	139
8.6	Asymptotic Analysis	140
8.6.1	Balanced Case	140
8.6.2	Unbalanced Case I	142
8.6.3	Unbalanced Case II	143
8.7	Numerical Results	143
8.8	Summary	150
9	Conclusion and Future work	167
9.1	Conclusion	167
9.2	Future work	170
	Bibliography	173
	Appendix	195

List of Figures

1.1	A basic system model of physical layer security: wiretap channel.	8
1.2	An illustrative figure depicting Beamforming mechanism.	11
3.1	System Model with a Friendly Jammer Beamforming to Eavesdropper	39
3.2	Secrecy rate vs. the source-to-eavesdropper distance, with path loss exponent as the parameter	44
3.3	Secrecy rate vs. the jammer-to-destination distance, with path loss exponent as the parameter.	45
3.4	Secrecy rate vs. PLE when the position of eavesdropper is varied.	46
3.5	Secrecy rate when the coordinates of eavesdropper is varied.	46
3.6	Secrecy rate when the coordinates of eavesdropper is varied, Rician shaping parameter $K = 5$ dB.	47
3.7	Secrecy rate when the coordinates of eavesdropper is varied, for Nakagami- m channel with $m = 1.5$	48
4.1	System Model with a Friendly Jammer	52
4.2	Data points generated from experiment and the cubic fit for PDF	55
4.3	ERJ corresponding to real, unequal roots of source power for dif- ferent location of jammer	64
4.4	ERJ corresponding to real, unequal roots of source power for dif- ferent path loss exponent	66
4.5	ERJ corresponding to real, unequal roots of source power for dif- ferent path loss exponent	67

4.6	ERJ corresponding to real, equal roots of source power for different position of jammer	68
4.7	ERJ corresponding to real, unequal roots of source power for different position of jammer	69
5.1	System model of a Hybrid Relaying Scheme	72
5.2	Comparison of Secrecy Outage Probability of AF, DF under balanced case.	79
5.3	Comparison of SOP of AF, DF, HDAF scheme under balanced case.	80
5.4	Comparison of SOP of AF, DF, HDAF scheme under balanced case, varying γ_{th}	80
5.5	Comparison of SOP of HDAF under different SNR unbalance condition.	81
6.1	System Model of two-hop AF relay network with single eavesdropper	86
6.2	Secrecy outage probability versus transmitted SNR(dB) ; $R_0 = 2$ BPCU	96
6.3	Secrecy outage probability versus x-axis of eavesdropper location ; $R_0 = 2$ BPCU	97
7.1	System model for dual-hop DF relay system with an eavesdropper. .	102
7.2	SOP comparison of MRC and SC diversity combining techniques in the balanced case.	123
7.3	SOP by varying γ_{th} in balanced case.	124
7.4	SOP when unbalance is created for a given $1/\beta_{sr}$	125
7.5	SOP when unbalance is created for a given $1/\beta_{rd}$	126
7.6	ESR for unbalanced case I and unbalanced case II.	127
8.1	System Model with a DF relay and Direct Link to Destination, Eavesdropper	132
8.2	SOP comparison of various diversity combining techniques under CSI and NOCSI scenario in the balanced case	144

8.3	SOP comparison of MRC-MRC schemes under NOCSI scenario in the balanced case	145
8.4	SOP of MRC-MRC schemes by varying γ_{th} under balanced case . . .	146
8.5	SOP of MRC-MRC scheme when unbalance is created for a given $1/\beta_{sr}$ and $1/\beta_{rd}$	147
8.6	ESR of MRC-SC and SC-MRC schemes for CSI scenario under balanced case	148
8.7	ESR for unbalance case I and II for $1/\beta_{sr} = 30$ dB and $1/\beta_{rd} = 30$ dB.	149

List of Tables

6.1	Secrecy Outage Probability of Different Relay Selection Schemes . . .	95
7.1	ESR of Various Combination of Diversity Combining Schemes at E When No Knowledge of CSI Available	114
7.2	ESR of Various Combination of Diversity Combining Schemes at E when complete knowledge of CSI is available	115
8.1	SOP of Various Combination of Diversity Combining Schemes at D and E when CSI is not available at the Transmitter from (8.12) . . .	151
8.2	SOP of Various Combination of Diversity Combining Schemes at D and E when CSI is available at the Transmitter from (8.17)	153
8.3	Ergodic Secrecy Rate of Various Diversity Combining Schemes at D and E	155
8.4	Asymptotic SOP under Balanced Case	159
8.5	Asymptotic SOP of Various Combination of Diversity Combining Schemes at D and E under Unbalanced Case I (when $1/\beta_{sr}$ is fixed and $1/\beta_{rd} = 1/\beta \rightarrow \infty$)	161
8.6	Asymptotic SOP under Unbalanced Case II (when $1/\beta_{rd}$ is fixed and $1/\beta_{sr} = 1/\beta \rightarrow \infty$)	163

List of Abbreviations

AF	Amplify-and-Forward
AN	Artificial Noise
AS	Asymptotic
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPCU	Bits Per Channel Use
CCI	Co-Channel Interference
CJ	Cooperative Jamming
CR	Cognitive Radio
CS	Conventional Selection
CS-J	Conventional Selection with Jamming
CS-NJ	Conventional Selection without Jamming
CSI	Channel State Information
DAF	Decode-Amplify-and-Forward
dB	Decibel
DF	Decode-and-Forward
DSC	Distributed Selection Combining
DSSC	Distributed Switch-and-Stay Combining
EGC	Equal Gain Combining
ERFR	Effective Region For Relaying
ESR	Ergodic Secrecy Rate
GSVD	Generalised Singular Value Decomposition
HDAF	Hybrid Decode-Amplify-and-Forward
IID	Independent and Identically Distributed
INID	Independent and Not Identically Distributed
IoT	Internet of Things

Table 1 – *Continued from previous page*

ISI	Inter Symbol Interference
LOS	Line-of-Sight
MGF	Moment Generating Function
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MMSE	Minimum Mean Square Error
MRC	Maximal Ratio Combining
MRT	Maximal Ratio Transmission
NF	Noise Forwarding
NOD	NO Direct link available
OFDMA	Orthogonal Frequency Division Multiple Access
OS	Optimal Selection
OSI	Open Systems Interconnection
PDF	Probability Density Function
PLE	Path Loss Exponent
PLS	Physical Layer Security
QoS	Quality of Service
RV	Random Variable
SC	Selection Combining
SDC	Selection Diversity Combining
SER	Symbol Error Rate
SISO	Single-Input Single-Output
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SRM	Secrecy Rate Maximization
SS	Suboptimal Selection
STBC	Space Time Block Code
TC	Threshold Combining

Table 1 – *Continued from previous page*

TH	Threshold
TPM	Transmit Power Minimization
ZF	Zero Forcing
